Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 2.0, Released on 2017-10-17

Document History

Date	Version	Editor	Description
2017-10-16	1.0	Daniel Gattringer	Initial version

Table of Contents

1. Purpose of the Technical Safety Concept

The creation of a technical safety concept is part of the safety process of ISO 26262 for the treatment of potential malfunctions in electrical and electronic systems.

The purpose of the technical safety concept is to transform functional safety requirements to additional technical requirements and allocate these high-level hardware and software requirements to system diagrams of the lane assistance functional safety project.

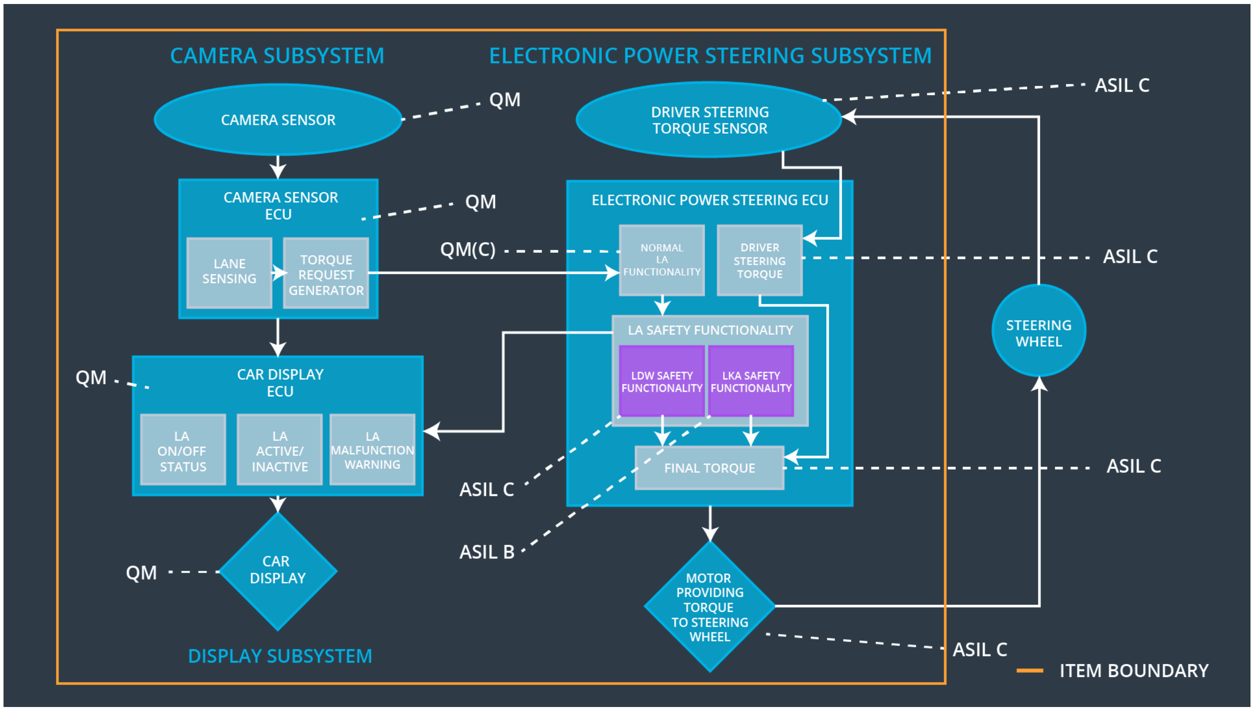
2. Inputs to the Technical Safety Concept

2.1. Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Set the oscillating torque to zero.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50ms	Set the oscillating torque to zero.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500ms	Set the lane keeping add extra torque to zero.
Functional Safety Requirement 03-01	The lane keeping item shall ensure that the lane departure warning by means of vibration of the steering wheel is only possible when LDW_On is set.	A	50ms	Set the oscillating torque to zero.
Functional Safety Requirement 04-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU can’t reliably detect the lane boundaries.	A	50ms	Set the lane keeping add extra torque to zero.
Functional	The electronic power steering ECU shall	A	50ms	Set the lane

Safety Requirement 04-02	ensure that the lane keeping assistance functionality is deactivated and signalized on the car display when the camera sensor ECU can’t reliably detect the lane boundaries.			keeping add extra torque to zero.

2.2. Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Sensor for the optical detection of the front area of the vehicle, including detectable lane lines.
Camera Sensor ECU	Electronic Control Unit responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Responsible for triggering reactions to add extra torque for LDW and LKA functionality.
Camera Sensor ECU Lane Sensing	Component within the camera sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Camera Sensor ECU Torque Request Generator	Component within the camera sensor ECU responsible for calculating and sending an request for additional steering torque for the LDW and LKA functionality.

Car Display	Visual display which is, among other functionalities, responsible for displaying warning of lane departures and LKA and LDW activation-status.
Car Display ECU	Electronic control unit, which is responsible for creating and providing the data and information that the car display visualizes.
Car Display ECU LA on/off status	Component within the car display ECU responsible for visualizing if the lane assistance functionality is switched on or off.
Car Display ECU LA active/inactive	Component within the car display ECU responsible for visualizing if the lane assistance functionality is active at the moment. Active means the car is drifting away from the center of the lane and LKA is actively acting or the car is getting too narrow to a lane boundary and LDW is warning.
Car Display ECU LA malfunction warning	Component within the car display ECU responsible for visualizing if there occurs any malfunction within the lane assistance system.
Driver Steering Torque Sensor	Sensor responsible for measuring the steering torque provided by the driver.
Electronic Power Steering (EPS) ECU	The electronic control unit is responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW).
EPS ECU Normal Lane Assistance Functionality	Component within the electronic power steering ECU responsible for receiving extra torque request from the camera sensor ECU and doing different non-safety tasks.
EPS ECU Driver Steering Torque	Component within the electronic power steering ECU responsible for receiving the steering torque with which the driver moves the steering wheel.
EPS ECU LDW Safety Functionality	Component within the electronic power steering ECU responsible for keeping the lane departure warning action (oscillating torque) below Max_Torque_Amplitude and Max_Torque_Frequency. This component is also responsible for ensuring that the lane departure warning by means of vibration of the steering wheel is only applicated when LDW_On is set.
EPS ECU LKA Safety Functionality	Component within the electronic power steering ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max_Duration to the center of the lane.

	This component is also responsible for ensuring that the lane keeping assistance by forcing the car to the center of the lane is only applicated when the lane boundaries can be detected reliably.
EPS ECU Final Torque	Component within the electronic power steering ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor.
Motor	Mechatronic device which adds extra steering torque directly to the steering wheel.

3. Technical Safety Concept

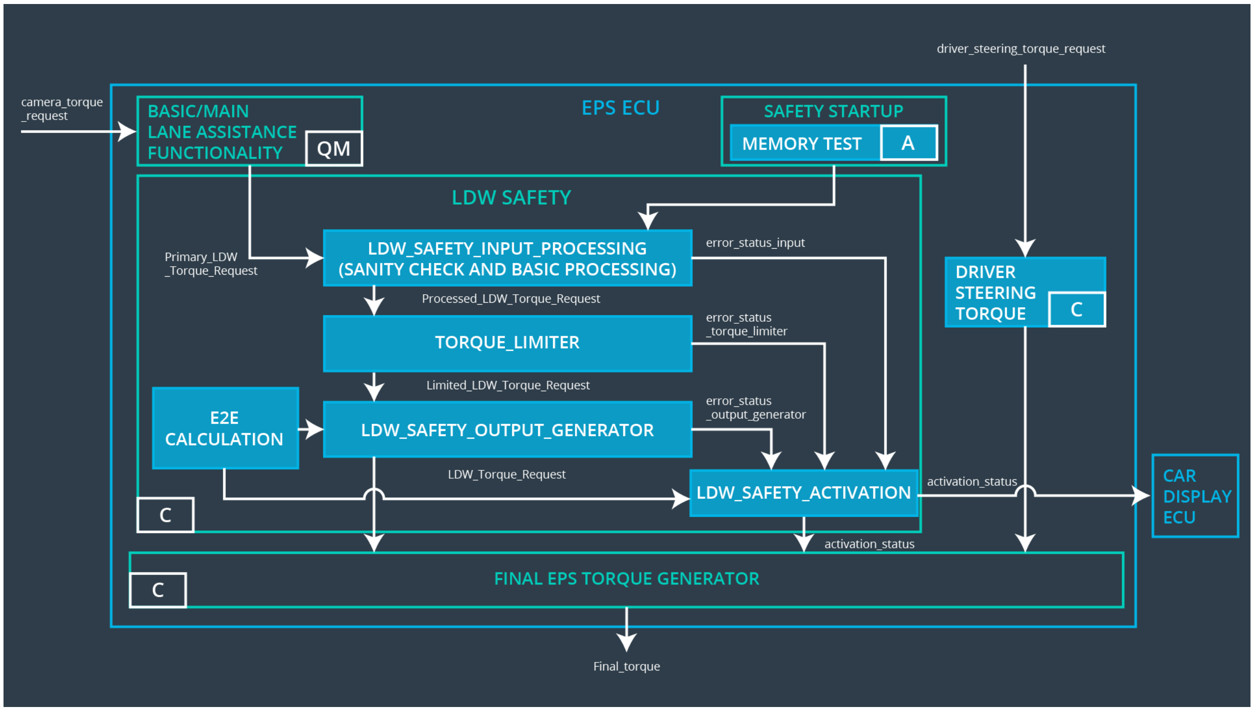
3.1. Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements
(derived in the functional safety concept):

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	X		

The following image shows the LDW safety component of the EPS ECU:


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

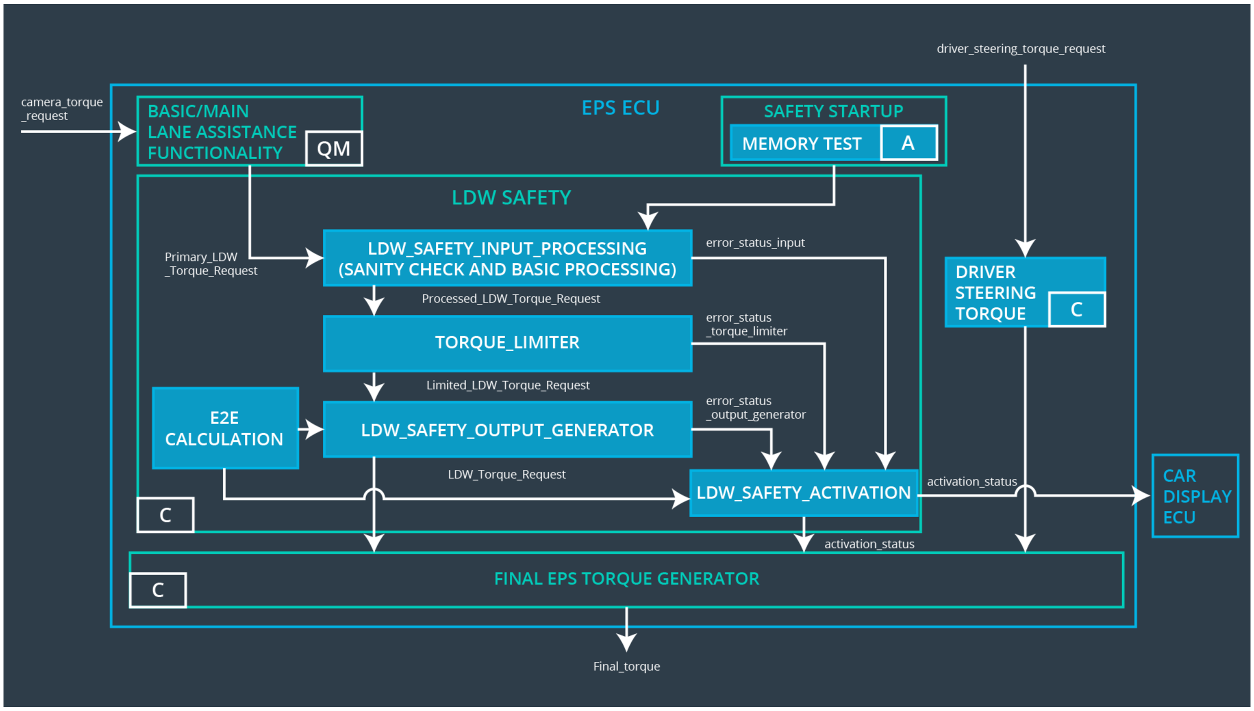
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Amplitude’	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.

Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50ms	EPS ECU – Data Transmission Integrity Check	Set the oscillating torque to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup	Set the oscillating torque to zero.

Functional Safety Requirement 01-02 with its associated system elements (derived in the functional safety concept):

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

The following image shows the LDW safety component of the EPS ECU:



driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
DRIVER STEERING TORQUE
C
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the frequency of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency.	C	50ms	EPS ECU - LDW Safety Component	Set the oscillating torque to zero.

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

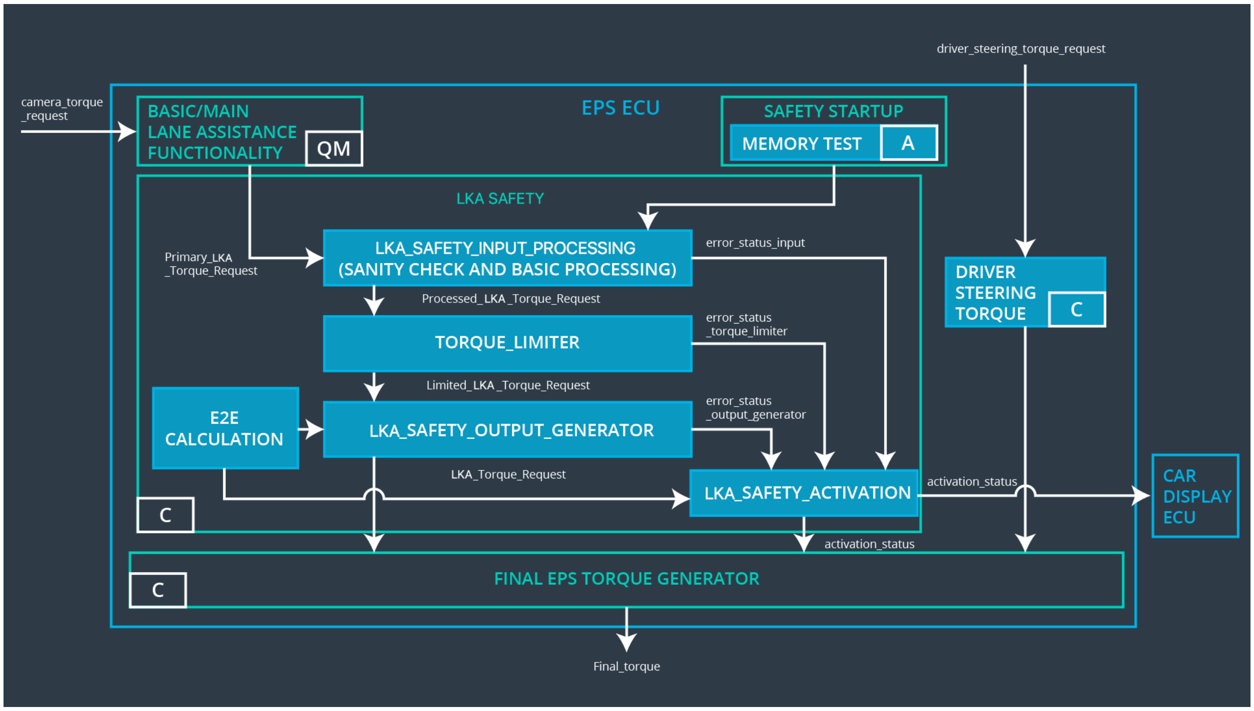
ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	Validate that Max_Torque_Amplitude is chosen high enough that the driver notices it but low enough not to cause loss of steering.	Verify that the LDW safety component really sets ‘LDW_Torque_Request’ to zero if the lane departure warning functionality ever causes a ‘LDW_Torque_Request’ with an amplitude above ‘Max_Torque_Amplitude’.
Technical Safety Requirement 01-01-02	Validate that the warning light for a deactivated LDW feature can be clearly recognized by the driver and is interpreted correctly.	Verify that the LDW safety component really sends a signal to the car display ECU to turn on a warning light every time the LDW function deactivates the LDW feature.
Technical Safety Requirement 01-01-03	Validate that the deactivation of the LDW feature and the absence of a vibration warning (in the steering wheel) when leaving the lane will not unsettle the driver and thus distract him.	Verify that the LDW safety component really deactivates the LDW feature and sets the ‘LDW_Torque_Request’ to zero every time it detects a failure.
Technical Safety Requirement 01-01-04	-	Verify that the Data Transmission Integrity component really checks the validity and integrity of the data transmission for the ‘LDW_Torque_Request’ signal every time it is sent.
Technical Safety Requirement 01-01-05	-	Verify that the Safety Startup component really checks the memory for any faults every time the EPS ECU is start up.
Technical Safety Requirement 01-02-01	Validate that Max_Torque_Frequency is chosen high enough that the driver notices it but low enough not to cause loss of steering.	Verify that the LDW safety component really sets ‘LDW_Torque_Request’ to zero if the lane departure warning functionality ever causes a ‘LDW_Torque_Request’ with an frequency above ‘Max_Torque_Frequency.

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-01 with its associated system elements
(derived in the functional safety concept):

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration.	X		

The following image shows the LKA safety component of the EPS ECU:


driver_steering_torque_request
camera_torque _request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LKA SAFETY
Primary_LKA _Torque_Request
LKA_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LKA_Torque_Request
error_status _torque_limiter
TORQUE_LIMITER
Limited_LKA_Torque_Request
E2E CALCULATION
error_status _output_generator
LKA_SAFETY_OUTPUT_GENERATOR
LKA_Torque_Request
LKA_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement	The LKA safety component shall ensure that the duration of the lane keeping assistance	C	500ms	EPS ECU - LKA Safety Component	Set the lane keeping add extra torque

02-01-01	torque applied is less than Max_Duration.				to zero.
Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light.	C	500ms	EPS ECU - LKA Safety Component	Set the lane keeping add extra torque to zero.
Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ‘LKA_Torque_Request’ shall be set to zero.	C	500ms	EPS ECU - LKA Safety Component	Set the lane keeping add extra torque to zero.
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	C	500ms	EPS ECU – Data Transmission Integrity Check	Set the lane keeping add extra torque to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup	Set the lane keeping add extra torque to zero.

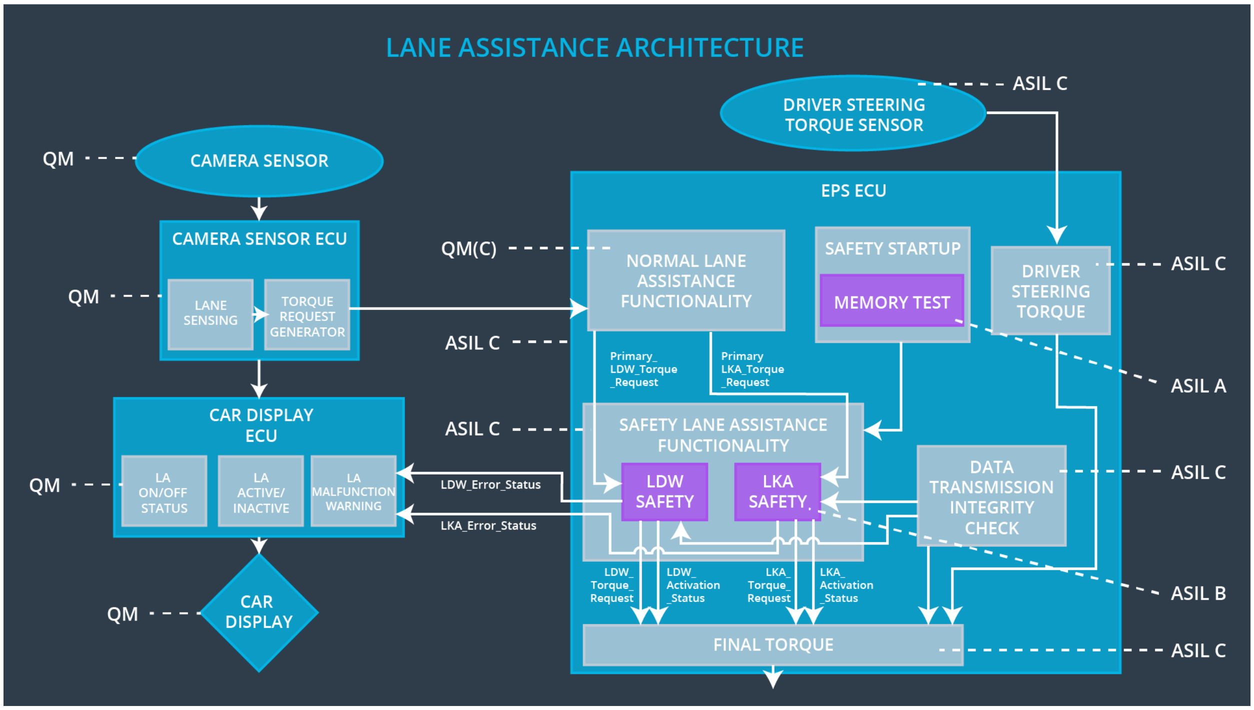
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-01-01	Validate the allowed usage time of the LKA feature ‘Max_Duration’ is long enough that it helps the driver to keep within the lane but it is too short to make the driver use the functionality for autonomous driving.	Verify that the LKA safety component really ensures that the LKA feature cannot be used longer than ‘Max_Duration’, without adding steering torque from the driver.
Technical Safety Requirement 02-01-02	Validate that the warning light for a deactivated LKA feature can be clearly recognized by the driver and is interpreted correctly.	Verify that the LKA safety component really sends a signal to the car display ECU to turn on a warning light every time the LKA function deactivates the LKA feature.
Technical Safety Requirement	Validate that the deactivation of the LKA feature and the absence of added steering torque when leaving the lane	Verify that the LKA safety component really deactivates the LKA feature and sets the ‘LKA_Torque_Request’ to

02-01-03	will not unsettle the driver and thus distract him.	zero every time it detects a failure.
Technical Safety Requirement 02-01-04	-	Verify that the Data Transmission Integrity component really checks the validity and integrity of the data transmission for the 'LKA_Torque_Request' signal every time it is sent.
Technical Safety Requirement 02-01-05	-	Verify that the Safety Startup component really checks the memory for any faults every time the EPS ECU is start up.

3.2. Refinement of the System Architecture

The following images shows the refined system architecture:



Technical overview of architecture elements:

Element	Description
Camera Sensor	Sensor for the optical detection of the front area of the vehicle, including detectable lane lines.
Camera Sensor ECU	Electronic Control Unit responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.

	Responsible for triggering reactions to add extra torque for LDW and LKA functionality.
Camera Sensor ECU Lane Sensing	Component within the camera sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Camera Sensor ECU Torque Request Generator	Component within the camera sensor ECU responsible for calculating and sending an request for additional steering torque for the LDW and LKA functionality.
Car Display	Visual display which is, among other functionalities, responsible for displaying warning of lane departures and LKA and LDW activation-status.
Car Display ECU	Electronic control unit, which is responsible for creating and providing the data and information that the car display visualizes.
Car Display ECU LA on/off status	Component within the car display ECU responsible for visualizing if the lane assistance functionality is switched on or off.
Car Display ECU LA active/inactive	Component within the car display ECU responsible for visualizing if the lane assistance functionality is active at the moment. Active means the car is drifting away from the center of the lane and LKA is actively acting or the car is getting too narrow to a lane boundary and LDW is warning.
Car Display ECU LA malfunction warning	Component within the car display ECU responsible for visualizing if there occurs any malfunction within the lane assistance system.
Driver Steering Torque Sensor	Sensor responsible for measuring the steering torque provided by the driver.
Electronic Power Steering (EPS) ECU	The electronic control unit is responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW).
EPS ECU Normal Lane Assistance Functionality	Component within the electronic power steering ECU responsible for receiving extra torque request from the camera sensor ECU and doing different non-safety tasks.
EPS ECU Driver Steering Torque	Component within the electronic power steering ECU responsible for receiving the steering torque with which the driver moves the steering wheel.
EPS ECU LDW Safety Functionality	Component within the electronic power steering ECU responsible for keeping the lane departure warning action

	(oscillating torque) below Max_Torque_Amplitude and Max_Torque_Frequency. This component is also responsible for ensuring that the lane departure warning by means of vibration of the steering wheel is only applicated when LDW_On is set.
EPS ECU LKA Safety Functionality	Component within the electronic power steering ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max_Duration to the center of the lane. This component is also responsible for ensuring that the lane keeping assistance by forcing the car to the center of the lane is only applicated when the lane boundaries can be detected reliably.
EPS ECU Final Torque	Component within the electronic power steering ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor.
EPS ECU Safety Startup Memory Test	Component within the electronic power steering ECU responsible for the memory test conducted at startup of the EPS ECU to check for any faults in memory.
EPS ECU Data Transmission Integrity Check	Component within the electronic power steering ECU responsible for checking the data validity and integrity of the data transmission.
Motor	Mechatronic device which adds extra steering torque directly to the steering wheel.

3.3. Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Amplitude’.	X		
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light.	X		
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero.	X		
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	X		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	X		
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the frequency of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency.	X		
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration.	X		

Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light.	**X**		
Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ‘LKA_Torque_Request’ shall be set to zero.	**X**		
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	**X**		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	**X**		

3.4. Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off LDW functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes, LDW oscillating torque shall be set to zero	Lane assistance functionality set inactive and malfunction warning to the driver via car display.
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_05	Yes, LKA added extra torque shall be set to zero	Lane assistance functionality set inactive and malfunction warning to the driver via car display.